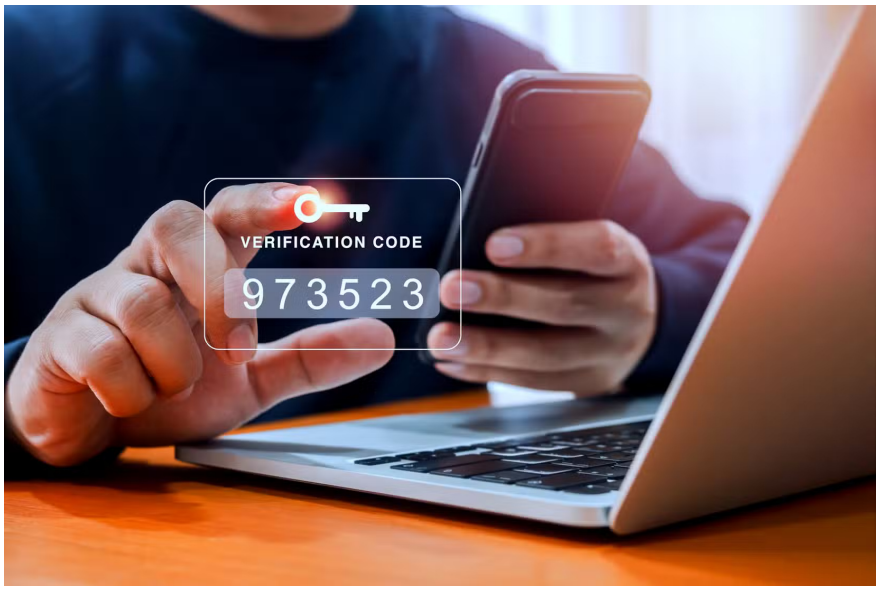
Here's What Hackers Hope You Never Do With Your Email!

There are a number of settings you can set to prevent your email from being hacked. However, if these settings are disabled, it can make a hacker a bargain, but ruin your day.

There are a number of settings you can set to prevent your email from being hacked. However, if these settings are disabled, it can make a hacker a bargain, but ruin your day.

Passwords Aren't Enough: Multi-Factor Authentication (MFA) Can Protect You From Hackers!

Believe it or not, passwords are the bane of the Internet . Easy-to-remember passwords that the average person might use for their accounts aren't very secure, while secure passwords are often not so easy to remember. This leaves us with a situation where most of the passwords we use every day, like passwords for our email inboxes, aren't very secure.



With computers getting faster and faster, brute-force attacks are less of a problem. Hackers often research their targets, making it easier to guess passwords. Account passwords are also often leaked in data breaches, and since

people tend to use the same password for multiple online accounts, this puts multiple accounts at risk from a single breach.

We can't eliminate passwords completely. However, they're also not the most secure authentication method and require additional verification. This is where Multi-Factor Authentication (MFA) comes in. MFA typically works by sending a one-time password (OTP) code to another account or device you own. Authenticator apps can generate these codes and are better protected against SIM swapping attacks, while SMS Two-Factor Authentication (2FA) is popular but not considered secure.

Essentially, it locks down your account using multiple 'factors.' In most cases, these factors are 'something you know,' such as a password, and 'something you have,' such as a phone that receives or generates OTPs. This is called two-factor authentication, or 2FA, and is the most common form of MFA you'll encounter online.

Having to enter a secondary code during login that only you have access to significantly reduces the risk of hackers getting your password. Whether they steal your password from a data breach or a phishing attack , they will still ask for an OTP. These codes are much harder to get unless the hacker has physical access to your phone.

How to enable MFA on email accounts

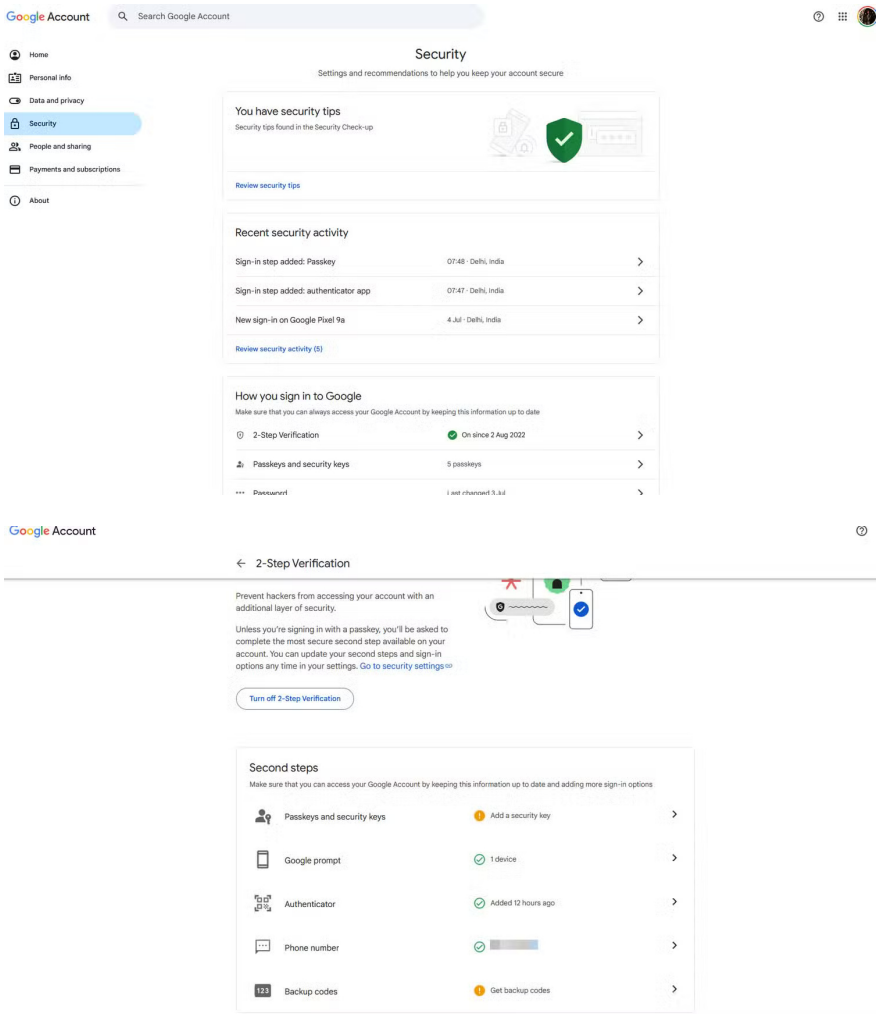
Most email services either require MFA or will prompt you to set it up. The steps to enable MFA vary depending on the email provider you're using, but you'll generally find the MFA settings hidden in your account's security and privacy settings.

TipsMake.com has covered how to secure your Gmail , Outlook , and other accounts with 2FA before, but here's a quick guide on how to enable the feature on some of the most popular email services.

Gmail

Enabling 2FA on Gmail is as simple as updating your Google account settings.

1. Go to your Google account, sign in and click on the **Security** tab .
2. Scroll down and click **2-Step Verification** . You may be prompted to sign in again.
3. Choose the login option that best suits your needs.

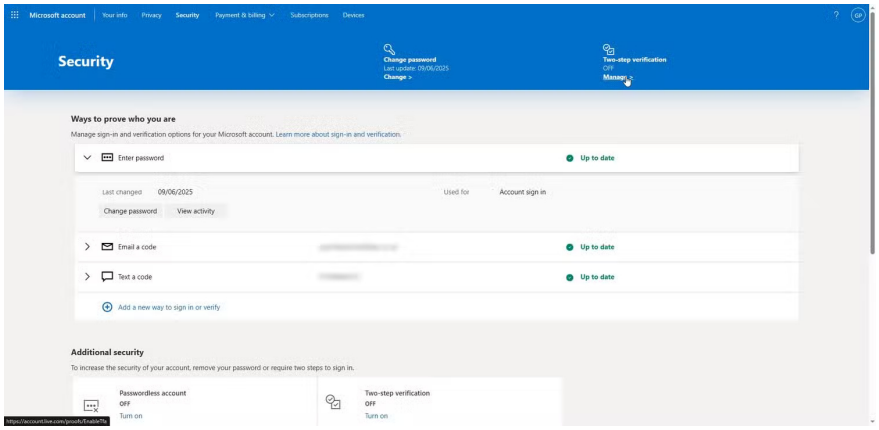


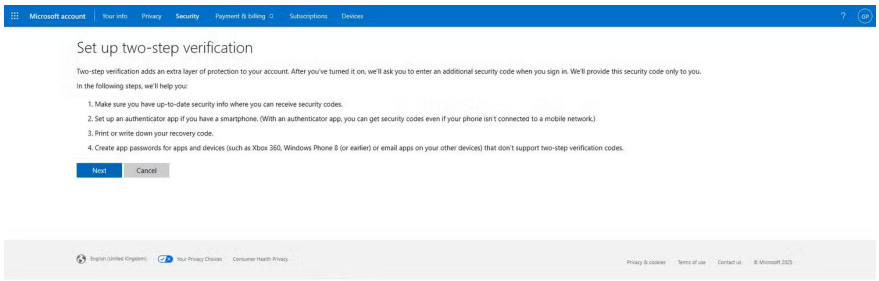
While Google can send OTPs via SMS, you should install Google Authenticator to generate OTPs locally on your device. The app is available on both Android and iOS and can also work with other services.

Outlook.com

You can also set up 2FA protection on Outlook.com. Note that this option is different from the Outlook desktop client.

1. Go to your Microsoft account page, then go to **Security** .
2. **Select the Two-step Verification** option , then select **Turn on two-step verification** and click **Next** to continue.
3. From here, you can set up your authenticator app to work with Outlook.com.



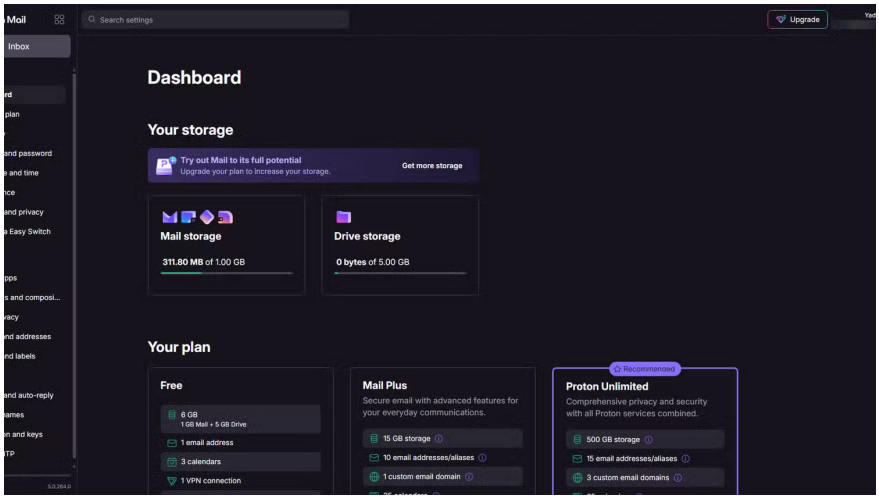


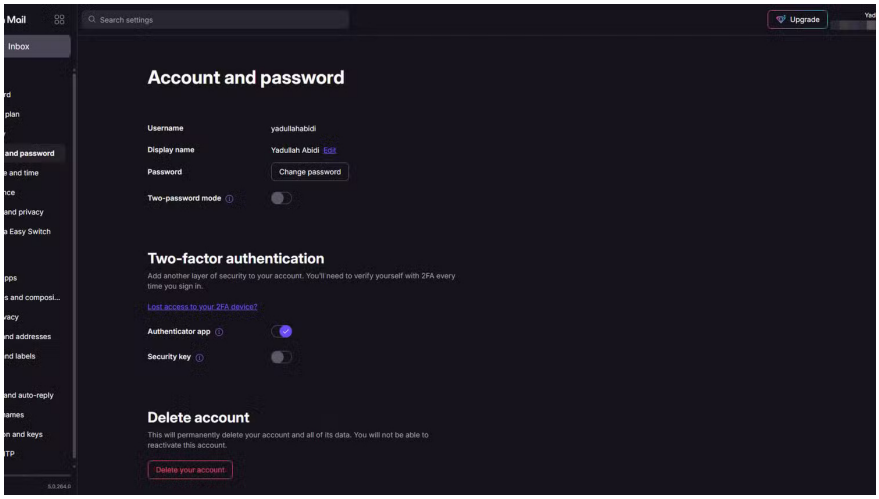
Other 2FA methods are set up using the email account and phone number associated with your account.

Proton Mail

Follow these steps to enable 2FA on Proton Mail.

1. Go to your Proton Mail dashboard, log in and click on **the Account and Password** tab .
2. Under **Two-factor authentication , turn on the Authenticator app** slider .
3. You will see a QR code . Scan the code with Google Authenticator to enable 2FA.





We have more online accounts than ever before, which means we're at greater risk of having our information exposed. With data breaches happening all the time, taking the time to secure your accounts with multi-factor authentication is a quick and easy way to add extra protection to your accounts.

You finished reading the article "**Here's What Hackers Hope You Never Do With Your Email!**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.